Notice of Allowability	Application No. 10/849,818	Applicant(s) SANDHU ET AL.	
	Examiner Ronald Baum	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *4/29/05*.

2. ☒ The allowed claim(s) is/are *1-18*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 12282005
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *12282005*.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Alfred Stadnicki, Reg. No. 30,226 on 1/3/2006.

1. Replace claims 1,9,10,17 with the following (shown ***marked up*** here, followed by *clean version*):

1. A system for accessing multiple different network stations without entry of a password, comprising:

a first network station

representing a network entity and

configured to

transmit a request for authentication of a user seeking access,

the user having

an associated password,

an associated user identifier, and

an associated asymmetric crypto-key, including

a first private key portion

obtainable with the password,

a second private key portion and

a public key portion;

a second network station

representing the user, and

having

the user identifier,

a combination symmetric crypto-key corresponding to

a first symmetric crypto-key and

a second symmetric crypto-key, and

the obtained first private key portion

encrypted with

the first symmetric crypto-key stored thereat, and

configured to

(i) transmit

the stored user identifier [MAC'd] message authenticated coded

with

the stored combination symmetric crypto-key responsive to

the transmitted authentication request, and

(ii) transmit

the transmitted authentication request

encrypted with

the stored combination symmetric crypto-key; and

a third network station,

representing a sponsor,

having

the user identifier,

the combination symmetric crypto-key,

the first symmetric crypto-key, and

the second private key portion stored thereat, and

configured to

(i) retrieve

the stored combination symmetric crypto-key by matching

the transmitted user identifier with

the stored user identifier,

(ii) verify

the MAC with

the retrieved combination symmetric crypto-key to

verify identity of the user,

(iii) decrypt

the transmitted encrypted authentication request with

the retrieved combination symmetric crypto-key to

recover the authentication request,

(iv) encrypt

the recovered authentication request with

the stored second private key portion and

(v) transmit

the encrypted authentication request and

the first symmetric crypto-key,

both encrypted with

the retrieved combination symmetric crypto-key;

wherein the second network station is further configured to

(i) decrypt

the transmitted encrypted authentication request and

first symmetric crypto-key, with

the stored combination symmetric crypto-key

to recover

the encrypted authentication request and

the first symmetric crypto-key,

(ii) decrypt

the stored encrypted first private key portion with

the recovered first symmetric crypto-key

to recover

the first private key portion,

(iii) to transmit

the recovered encrypted authentication request further

encrypted with

the recovered first private key portion; and

wherein the first station is further configured to

decrypt the transmitted further encrypted authentication request with

the public key

to thereby authenticate the user.

9. A system for accessing multiple different network stations, comprising:

a first station

representing a user

having

a password,

an identifier, and

an asymmetric crypto-key, including

a first private key portion,

a second private key portion and

a public key portion, and

configured

to transmit a log-in request including

the user identifier; and

a second station

representing a sponsor and

configured

to transmit a challenge responsive to

the transmitted log-in request;

wherein the first station is further configured

(i) to process the user password

to obtain the first private key portion,

(ii) to encrypt

a first symmetric crypto-key and

the transmitted challenge with

the obtained first private key portion

to form a first encrypted message, and

(iii) to transmit the first encrypted message;

wherein the second station is further configured

(i) to decrypt

the transmitted first encrypted message with

the second private key portion

to recover

the challenge and

the first symmetric crypto-key,

thereby authenticating the user,

(ii) to combine

the recovered first symmetric crypto-key with

a second symmetric crypto-key

to form a combined symmetric crypto-key,

(iii) to store the combined symmetric crypto-key,

(iv) to encrypt

the second symmetric crypto-key and

a time value with the first symmetric crypto-key

to form a second encrypted message, and

(v) to transmit the second encrypted message;

wherein the first station is further configured

(i) to decrypt

the transmitted second encrypted message with

the first symmetric crypto-key

to recover

the second symmetric crypto-key and

the time value,

thereby authenticating the sponsor,

(ii) to combine

the recovered second symmetric crypto-key with

the first symmetric crypto-key

to form the combined symmetric crypto-key,

(iii) to encrypt

the first private key portion with

the first symmetric crypto-key,

(iv) to destroy

the first symmetric crypto-key and

the obtained first private key portion,

(v) to encrypt

a request for user authentication from another network entity with

the combined symmetric crypto-key

to form a third encrypted message and

(vi) to transmit

the user identifier,

[MAC'd] message authenticated coded with

the combined symmetric crypto-key, and

the third encrypted message;

wherein the second station is further configured

(i) to match

the transmitted user identifier with

the previously transmitted user identifier

to retrieve the combined symmetric crypto-key,

(ii) verify

the MAC with

the retrieved combined symmetric crypto-key

to verify identity of the user,

(iii) to decrypt

the third encrypted message with

the combined symmetric crypto-key

to recover the request for user authentication,

(iv) to encrypt

the request for user authentication with

the second private key portion

to form a fourth encrypted message,

(v) to encrypt

the first symmetric crypto-key and

the fourth encrypted message with

the combined symmetric crypto-key

to form a fifth encrypted message and

(vi) to transmit the fifth encrypted message;

wherein the first network station is further configured

(i) to decrypt

the transmitted fifth encrypted message with

the combined symmetric crypto-key

to recover

the transmitted first symmetric crypto-key and

the transmitted fourth encrypted message, and

thereby verify an identity of the sponsor,

(ii) to decrypt

the encrypted first private key portion with

the recovered first symmetric crypto-key,

(iii) to further encrypt

the recovered fourth encrypted message with

the decrypted first private key portion

to form an authentication message,

(iv) to transmit the authentication message to

the other network entity

to authenticate the user.

10. A method for accessing multiple different network stations without entry of a password associated with a user also having an associated identifier and an associated asymmetric crypto-key, including a first private key portion obtainable with the password, a second private key portion and a public key portion, comprising:

receiving a request for authentication of the user;

retrieving from a first memory,

without entry of the user password,

the user identifier,

a combination symmetric crypto-key corresponding to

a first symmetric crypto-key and

a second symmetric crypto-key, and

the first private key portion

encrypted with

the first symmetric crypto-key;

encrypting

the transmitted authentication request with

the retrieved combination symmetric crypto-key;

transmitting

the retrieved user identifier

[MAC'd] message authenticated coded with

the retrieved combination symmetric crypto-key, and

the received authentication request

encrypted with

the retrieved combination symmetric crypto-key;

matching

the transmitted user identifier with

a user identifier stored in a second memory, different than the first memory,

to retrieve the combination symmetric crypto-key from the second memory;

verifying

the MAC with

the retrieved combination symmetric crypto-key

to verify identity of the user;

decrypting

the transmitted encrypted authentication request with

the combination symmetric crypto-key

to recover the authorization request;

retrieving

the second private key portion and

the first symmetric crypto-key from the second memory;

encrypting

the recovered authorization request with

the retrieved second private key portion

to form an authentication message;

transmitting

the authentication message and

the retrieved first symmetric crypto-key,

both encrypted with

the combination symmetric crypto-key;

decrypting

the transmitted encrypted authentication message and

first symmetric crypto-key, with

the combination symmetric crypto-key retrieved from the first memory

to recover

the authentication message and

the first symmetric crypto-key;

decrypting

the retrieved encrypted first private key portion with

the recovered first symmetric crypto-key;

encrypting

the recovered authentication message with

the decrypted first private key portion

to complete the authentication message;

transmitting the completed authentication message; and

decrypting

the transmitted completed authentication message with

the user public key to thereby authenticate the user.

17. A method for accessing multiple different network stations by a user having a user identifier, a user password and an asymmetric crypto-key, including a first private key portion, a second private key portion and a public key portion;

transmitting a log-in request including the user identifier;

transmitting

a challenge of a sponsor responsive

to the transmitted log-in request;

processing

the user password

to obtain the first private key portion;

encrypting

a first symmetric crypto-key and

the transmitted challenge with

the obtained first private key portion

to form a first encrypted message;

transmitting the first encrypted message;

decrypting

the transmitted first encrypted message with

the second private key portion

to recover

the challenge and

the first symmetric crypto-key, and

thereby authenticate the user to the sponsor;

combining

the recovered first symmetric crypto-key with

a second symmetric crypto-key

to form a combined symmetric crypto-key;

storing

the combined symmetric crypto-key

in a first memory;

encrypting

the second symmetric crypto-key with

the first symmetric crypto-key

to form a second encrypted message;

transmitting the second encrypted message;

decrypting

the transmitted second encrypted message with

the first symmetric crypto-key

to recover

the second symmetric crypto-key, and

thereby authenticate the sponsor to the user;

combining

the recovered second symmetric crypto-key with

the first symmetric crypto-key

to form the combined symmetric crypto-key;

storing

the combined symmetric crypto-key

in a second memory,

different than the first memory;

encrypting

the first private key portion with

the first symmetric crypto-key;

destroying

the first symmetric crypto-key used to encrypt the first private key portion and

the obtained first private key portion;

encrypting

a request for authentication of the user with

the combined symmetric crypto-key

to form a third encrypted message;

transmitting

the user identifier,

[MAC'd] message authenticated coded with

the combined symmetric crypto-key, and

the third encrypted message;

matching

the transmitted user identifier with

the previously transmitted user identifier

to retrieve the combined symmetric crypto-key from the second memory;

verifying

the transmitted MAC with

the retrieved combined symmetric crypto-key

to verify an identity of the user;

decrypting

the third encrypted message with

the combined symmetric crypto-key

to recover the request for user authentication;

encrypting

the request for user authentication with

the second private key portion

to form a fourth encrypted message;

encrypting

the first symmetric crypto-key and

the fourth encrypted message with

the combined symmetric crypto-key stored in the first memory

to form a fifth encrypted message;

transmitting the fifth encrypted message;

decrypting

the transmitted fifth encrypted message with

the combined symmetric crypto-key stored in the second memory

to recover

the transmitted first symmetric crypto-key and

the transmitted fourth encrypted message, and

thereby verify an identity of the sponsor;

decrypting

the encrypted first private key portion with

the recovered first symmetric crypto-key;

further encrypting

the recovered fourth encrypted message with

the decrypted first private key portion

to form an authentication message;

transmitting

the authentication message

to the other network entity

to authenticate the user.

Clean claim version:

1. A system for accessing multiple different network stations without entry of a password, comprising:

a first network station

representing a network entity and

configured to

transmit a request for authentication of a user seeking access,

the user having

an associated password,

an associated user identifier, and

an associated asymmetric crypto-key, including

a first private key portion

obtainable with the password,

a second private key portion and

a public key portion;

a second network station

representing the user, and

having

the user identifier,

a combination symmetric crypto-key corresponding to

a first symmetric crypto-key and

a second symmetric crypto-key, and

the obtained first private key portion

encrypted with

the first symmetric crypto-key stored thereat, and

configured to

(i) transmit

the stored user identifier message authenticated coded with

the stored combination symmetric crypto-key responsive to

the transmitted authentication request, and

(ii) transmit

the transmitted authentication request

encrypted with

the stored combination symmetric crypto-key; and

a third network station,

representing a sponsor,

having

the user identifier,

the combination symmetric crypto-key,

the first symmetric crypto-key, and

the second private key portion stored thereat, and

configured to

(i) retrieve

the stored combination symmetric crypto-key by matching

the transmitted user identifier with

the stored user identifier,

(ii) verify

the MAC with

the retrieved combination symmetric crypto-key to

verify identity of the user,

(iii) decrypt

the transmitted encrypted authentication request with

the retrieved combination symmetric crypto-key to

recover the authentication request,

(iv) encrypt

the recovered authentication request with

the stored second private key portion and

(v) transmit

the encrypted authentication request and

the first symmetric crypto-key,

both encrypted with

the retrieved combination symmetric crypto-key;

wherein the second network station is further configured to

(i) decrypt

the transmitted encrypted authentication request and

first symmetric crypto-key, with

the stored combination symmetric crypto-key

to recover

the encrypted authentication request and

the first symmetric crypto-key,

(ii) decrypt

the stored encrypted first private key portion with

the recovered first symmetric crypto-key

to recover

the first private key portion,

(iii) to transmit

the recovered encrypted authentication request further

encrypted with

the recovered first private key portion; and

wherein the first station is further configured to

decrypt the transmitted further encrypted authentication request with the public key

to thereby authenticate the user.

9. A system for accessing multiple different network stations, comprising:

a first station

representing a user

having

a password,

an identifier, and

an asymmetric crypto-key, including

a first private key portion,

a second private key portion and

a public key portion, and

configured

to transmit a log-in request including

the user identifier; and

a second station

representing a sponsor and

configured

to transmit a challenge responsive to

the transmitted log-in request;

wherein the first station is further configured

(i) to process the user password

to obtain the first private key portion,

(ii) to encrypt

a first symmetric crypto-key and

the transmitted challenge with

the obtained first private key portion

to form a first encrypted message, and

(iii) to transmit the first encrypted message;

wherein the second station is further configured

(i) to decrypt

the transmitted first encrypted message with

the second private key portion

to recover

the challenge and

the first symmetric crypto-key,

thereby authenticating the user,

(ii) to combine

the recovered first symmetric crypto-key with

a second symmetric crypto-key

to form a combined symmetric crypto-key,

(iii) to store the combined symmetric crypto-key,

(iv) to encrypt

the second symmetric crypto-key and

a time value with the first symmetric crypto-key

to form a second encrypted message, and

(v) to transmit the second encrypted message;

wherein the first station is further configured

(i) to decrypt

the transmitted second encrypted message with

the first symmetric crypto-key

to recover

the second symmetric crypto-key and

the time value,

thereby authenticating the sponsor,

(ii) to combine

the recovered second symmetric crypto-key with

the first symmetric crypto-key

to form the combined symmetric crypto-key,

(iii) to encrypt

the first private key portion with

the first symmetric crypto-key,

(iv) to destroy

the first symmetric crypto-key and

the obtained first private key portion,

(v) to encrypt

a request for user authentication from another network entity with

the combined symmetric crypto-key

to form a third encrypted message and

(vi) to transmit

the user identifier,

message authenticated coded with

the combined symmetric crypto-key, and

the third encrypted message;

wherein the second station is further configured

(i) to match

the transmitted user identifier with

the previously transmitted user identifier

to retrieve the combined symmetric crypto-key,

(ii) verify

the MAC with

the retrieved combined symmetric crypto-key

to verify identity of the user,

(iii) to decrypt

the third encrypted message with

the combined symmetric crypto-key

to recover the request for user authentication,

(iv) to encrypt

the request for user authentication with

the second private key portion

to form a fourth encrypted message,

(v) to encrypt

the first symmetric crypto-key and

the fourth encrypted message with

the combined symmetric crypto-key

to form a fifth encrypted message and

(vi) to transmit the fifth encrypted message;

wherein the first network station is further configured

(i) to decrypt

the transmitted fifth encrypted message with

the combined symmetric crypto-key

to recover

the transmitted first symmetric crypto-key and

the transmitted fourth encrypted message, and

thereby verify an identity of the sponsor,

(ii) to decrypt

the encrypted first private key portion with

the recovered first symmetric crypto-key,

(iii) to further encrypt

the recovered fourth encrypted message with

the decrypted first private key portion

to form an authentication message,

(iv) to transmit the authentication message to

the other network entity

to authenticate the user.

10. A method for accessing multiple different network stations without entry of a password associated with a user also having an associated identifier and an associated asymmetric crypto-key, including a first private key portion obtainable with the password, a second private key portion and a public key portion, comprising:

receiving a request for authentication of the user;

retrieving from a first memory,

without entry of the user password,

the user identifier,

a combination symmetric crypto-key corresponding to

a first symmetric crypto-key and

a second symmetric crypto-key, and

the first private key portion

encrypted with

the first symmetric crypto-key;

encrypting

the transmitted authentication request with

the retrieved combination symmetric crypto-key;

transmitting

the retrieved user identifier

message authenticated coded with

the retrieved combination symmetric crypto-key, and

the received authentication request

encrypted with

the retrieved combination symmetric crypto-key;

matching

the transmitted user identifier with

a user identifier stored in a second memory, different than the first memory,

to retrieve the combination symmetric crypto-key from the second memory;

verifying

the MAC with

the retrieved combination symmetric crypto-key

to verify identity of the user;

decrypting

the transmitted encrypted authentication request with

the combination symmetric crypto-key

to recover the authorization request;

retrieving

the second private key portion and

the first symmetric crypto-key from the second memory;

encrypting

the recovered authorization request with

the retrieved second private key portion

to form an authentication message;

transmitting

the authentication message and

the retrieved first symmetric crypto-key,

both encrypted with

the combination symmetric crypto-key;

decrypting

the transmitted encrypted authentication message and

first symmetric crypto-key, with

the combination symmetric crypto-key retrieved from the first memory

to recover

the authentication message and

the first symmetric crypto-key;

decrypting

the retrieved encrypted first private key portion with

the recovered first symmetric crypto-key;

encrypting

the recovered authentication message with

the decrypted first private key portion

to complete the authentication message;

transmitting the completed authentication message; and

decrypting

the transmitted completed authentication message with

the user public key to thereby authenticate the user.

17. A method for accessing multiple different network stations by a user having a user identifier, a user password and an asymmetric crypto-key, including a first private key portion, a second private key portion and a public key portion;

transmitting a log-in request including the user identifier;

transmitting

a challenge of a sponsor responsive

to the transmitted log-in request;

processing

the user password

to obtain the first private key portion;

encrypting

a first symmetric crypto-key and

the transmitted challenge with

the obtained first private key portion

to form a first encrypted message;

transmitting the first encrypted message;

decrypting

the transmitted first encrypted message with

the second private key portion

to recover

the challenge and

the first symmetric crypto-key, and

thereby authenticate the user to the sponsor;

combining

the recovered first symmetric crypto-key with

a second symmetric crypto-key

to form a combined symmetric crypto-key;

storing

the combined symmetric crypto-key

in a first memory;

encrypting

the second symmetric crypto-key with

the first symmetric crypto-key

to form a second encrypted message;

transmitting the second encrypted message;

decrypting

the transmitted second encrypted message with

the first symmetric crypto-key

to recover

the second symmetric crypto-key, and

thereby authenticate the sponsor to the user;

combining

the recovered second symmetric crypto-key with

the first symmetric crypto-key

to form the combined symmetric crypto-key;

storing

the combined symmetric crypto-key

in a second memory,

different than the first memory;

encrypting

the first private key portion with

the first symmetric crypto-key;

destroying

the first symmetric crypto-key used to encrypt the first private key portion and

the obtained first private key portion;

encrypting

a request for authentication of the user with

the combined symmetric crypto-key

to form a third encrypted message;

transmitting

the user identifier,

message authenticated coded with

the combined symmetric crypto-key, and

the third encrypted message;

matching

the transmitted user identifier with

the previously transmitted user identifier

to retrieve the combined symmetric crypto-key from the second memory;

verifying

the transmitted MAC with

the retrieved combined symmetric crypto-key

to verify an identity of the user;

decrypting

the third encrypted message with

the combined symmetric crypto-key

to recover the request for user authentication;

encrypting

the request for user authentication with

the second private key portion

to form a fourth encrypted message;

encrypting

the first symmetric crypto-key and

the fourth encrypted message with

the combined symmetric crypto-key stored in the first memory

to form a fifth encrypted message;

transmitting the fifth encrypted message;

decrypting

the transmitted fifth encrypted message with

the combined symmetric crypto-key stored in the second memory

to recover

the transmitted first symmetric crypto-key and

the transmitted fourth encrypted message, and

thereby verify an identity of the sponsor;

decrypting

the encrypted first private key portion with

the recovered first symmetric crypto-key;

further encrypting

the recovered fourth encrypted message with

the decrypted first private key portion

to form an authentication message;

transmitting

the authentication message

to the other network entity

to authenticate the user.

Examiner's Statement of Reasons for Allowance

2. Claims 1-18 are allowed over prior art.

3. This action is in reply to applicant's correspondence of 29 April 2005

4. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

5. As per claims 1,9,10,17,18, generally, prior art of record, Erfani, U.S. Patent 6,542,993 B1, Jablon, U.S. Patent Pub. US2002/0067832 A1, Panjwani, U.S. Patent Pub. US2002/0018569 A1, Jablon, U.S. Patent 6,226,383 B1, Weber et al, U.S. Patent 6,178,409 B1, Underwood, U.S. Patent 6,704,873 B1, Ginter et al, U.S. Patent 6,948,070 B1, Oracle, and Fu et al fails to teach alone, or in combination, other than hindsight, at the time of the invention, the claimed features and limitations. Generally, prior art of record deals with various authentication schemes/system management aspects (Erfani, Jablon, Weber et al, Underwood, Fu and Ginter et al) comprising encryption (public, symmetric, session/transaction oriented), hashing, MAC functions, and information token aspects of the communications of the authentication request/responses across various network architectures (i.e., the Internet). The encryption service (i.e., key generation/exchange, partial and key exchange in the entirety) aspects are taught in the prior art of record (Panjwani, Jablon, Oracle and Fu) such that the various protocols per se (i.e., PKI, session/SSL, etc.,) are generally taught in association to applications dealing with network

communications/security services, but, the combination of authentication, encryption, and network architecture limitations are not taught, or are in any way other than hindsight, obvious.

6. Dependent claims 2-8,11-16 are allowable by virtue of their dependencies.

Conclusion

7. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100